```
/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\/|\
\|/                                                       \|/
/|\                                                       /|\
\|/        An Indepth Guide in Hacking UNIX and the       \|/
/|\           concept of Basic Networking Utility         /|\
\|/        ----------------------------------------       \|/
/|\                   By:Red Knight                       /|\
\|/        Phreakers/Hackers Underground Network          \|/
/|\                                                       /|\
\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/\|/
```

Brief history on UNIX

Its because of Ken Tompson that today were able to Hack Unix.He used to work for Bell Labs in the 60s.Tompson started out using the MULTICS OS which was later eliminated and Tompson was left without an operating system to work with. Tompson had to come up with something real quick.He did some research and and in 1969 UNIX came out,which was a single user and it didn't have many capabilities.A combined effort with others he rewrote the version in C and added some good features.This version was out in 1973 and was available to the public.This was the first begining of UNIX as its known presently.The more refined version of UNIX,today know as UNIX system V developed by Berkley University has unique capabilities.
Various types of UNIXes are CPIX,Berkeley Ver 4.1,Berkeley 4.2,FOS,Genix,HP-UX, IS/I,OSx,PC-IX,PERPOS,Sys3,Ultrix,Zeus,Xenix,UNITY,VENIX,UTS,Unisys,Uniplus+, UNOS,Idris,QNIX,Coherent,Cromix,System III,System 7,Sixth edition.

The article it self:

I believe that hacking into any system requires knowledge of the Operating system itself.Basically what I will try to do is make you more familiar with UNIX operation ,its usefull commands that will be advantageous to you as a hacker.This article contains in depth explainations.

Error Messages that one may came across:[UNIX system V]

Login incorrect - An ivalid ID and/or pw was entered.This means nothing.
In UNIX there is no way guessing valid user IDs.You may
come across this one when trying to get in.
No more logins - will happens when the system wont accept anymore logins
could be going down
Unknown Id - will happen if an ivalid id is entered using (su) command
Unexpected eof in file - The file being stripped file has been damaged
Your password has expired - This is quiet rare although there have been cases
where it happened.Reading the etc/passwd will
show you at how many intervals it changes.
You may not change the password - The password has not yet aged enough.The
Administrator set the quotas for the users
Unknown group [groups name] - occurs when chgrp is executed ,group doesn't
exist
Sorry - Indicated that you have typed in an invalid super user password(execu-
tion of the su)
Permission denied!- Indicated you must be the owner or a super user to change
password.
Sorry <[# of weeks] since last change - This will happen when password has
has not aged enough and you tried to
change it(passwd)
[directory name]:no permission - You are trying to remove a directory which
you have no permission to.
[file name] not removed - trying to delete a file owned by another user
that you dont have write pemision for.
[dirname] not removed - ownership of the dir is not your that your trying to
delete.

```
[dirname] not empty - the directory contains files so you must have to delete
                      the files before executing the rmdir
[command] not found - you have entered an ivalid command not know to UNIX
cant execute pwd - some thing wrong with the system cant execute pwd command
cannot chdir to .. -   (.. one level up) permision is required to execute pwd
                       above the current directory
cant open [file name] - defined wrong path,file name or you have no read
                        permission
cp:[file name] and [file name] are identical - self explanatory
cannot locate parent directory - occurs when using mv
[file name] not found - file which your trying to move doesn't exsist
You have mail - Self explanatory
```

Basic Networking Utility error messages

```
cu:not found - networking not installed
login failed - invalid id/pw or wrong # specified
dial failed - the systen never answered due to a wrong #
uucp completely failed - did not specify file after -s
wrong time to call - you called at the time at a time not specified in the
                     Systems file
system not in systems - you called a remote not in the systems file
```

Logon format : first thing one must do is switch to lower case
---

Identifing a UNIX.Here is what you'll see:
Some times there will be no system identifer

AT&T UNIX SysVR3.0 (eg of a system identifier)

```
login:
 or
Login:
```

Any of these is a UNIX.Here is where you will have to guess at a user valid id.Here are some that I have come across eg(glr,glt,radgo,rml,chester,cat, lom,cora,hlto,hwill,edcasey and also some containing numbers smith1,mitu6 or special characters in it like bremer$,j#fox.Login names have to be 3 to 8 chracters in lenght lowercase and must start with a letter.In some XENIX systems one may login as "guest"

User level accounts:(lower case)

In Unix they have whats called accounts .These
accounts can be used at the "login:" prompt.
Here is a list:

```
sys
bin
trouble
daemon
uucp
nuucp
rje
lp
adm
listen - if starlan is installed
```

Super-user accounts:

And then there are super-user login which make UNIX worth hacking.
The accounts are used for a specific job. In large systems these logins
are assingned to users who have a responsibilty to maintain subsystems.

They are as follows :(all lower case)

```
root       -  this is a must the system comes configured with it.It has no
              restriction.Has power over every other account.
unmountsys -  unmounts files
setup      -  system set up
makefsys   -  makes a new file
sysadm     -  allows useful S.A commands(doesn't need root login)
powerdown  -  powering system down
mountfsys  -  mounts files
checkfsys  -  checks file
```

These accounts will definitly have passwords assigned to them.These accounts are also commands used by the system administrator.

Here are some examples of accounts I have seen:

```
cron         uuhelp     usenet
anonuccp     news       network
bellboy      lp         vector
guest        games      ninja
vote         warble     sysinfo
```

After the login prompt you will receive a password prompt:

```
password:
  or
Password:
```

Enter the password (it wont echo).The password rule is as follows:Each pw has to contain at least 6 characters and maximum has to be 8 .Two of which are to be alphabetic letters and at least one being a number or a special character The alphabetic digits could be in upper case or lower case.Here are some of the passwords that I have seen (eg.Ansuya1,PLAT00N6,uFo/78,ShAsHi..,Div417co)

The passwords for the super user accounts will be difficult to hack try the accounts interchangebly eg.login:sysadm password:makefsys or rje1, sysop,sysop1,bin4 or they might contain letter,numbers,special chracters in them.It could be anything.The user passwords are changed by an aging proccess at successive intervals.The users are forced to changed it.The super-user will pick a password that wont need changing for a long period of time.

You have made it!

The hard part is over and hopefully you have hacked a super-user account.
Remember Control-d stops a process and also logs you off.
The next thing you'll probably see is the system news
eg.

```
login:john
password:hacker1
System news
There will be no networking offered to the users till
august 15,due to hardware problems.
(just an example)

$
```

```
$ is the Unix prompt -waiting for a command to be entered.I will use this
                      throught the article to show outouts etc..(Its not
                      part of the command)
# - means your logged in as root(very good)
```

A word about the XENIX System III:(run on the tandy 6000)

The largest weakness in the XENIX System III occurs after the installation of the Profile-16 or more commonly know as the filepro-16.I have seen the filepro-16 installed in many systems.
The installation process creates an entry in the password file for a user named \fBprofile\fR ,an account that who owns and administors the database. The great thing about it is that when the account is created ,no password is assigned to it.The database contains executable to maintain it.The database creation programs perform a \fBsetuid\fR to boot up the \fBoot\fR there by giving a person the whole C Shell to gain Super User privilege same as root. Intresting huh!

* Note: First the article will inform you of how the Unix is made up

The Unix is made if three components-The shell,the kernal,file system.

The kernal:

You could say that the kernal is the heart of the Unix operating system. The kernal is a low level language lower than the shell which maintains processes .The kernal handles memory usage ,maintains file system the sofware and hardware devices.

The shell:

The shell a higher level language. The shell had two important uses, to act as command interpreture for example using commands like cat,who, ls the the shell is at work figuring out whether you have entered a command correctly or not.The second most important reason for the shell is its ability to be used as programing language.Suppose your performing some tasks repeatedly over and over again,You can program the shell to do this for you.

The file system:

The file system in Unix is divede into 3 catagories:Directories,ordinary files and special files.(d,-)

Basic stucture:
(/)-this is abreviation for the root dirctory.

```
  root level                      root
                                  (/)                                 system
-------------------------------------|-----------------------------------level
|      |        |         |                  |        |       |        |
/unix   /etc    /dev      /tmp               /lib     /usr    /usr2    /bin
        |                                        _____|_____
login passwd                                     |    |    |
level                                            /john  /cathy
                             ________________________|_______________
                            |        |     |      |        |        |
                        .profile   /mail  /pers  /games   /bin     /michelle
*.profile - in case                        |    __|______  |      __|_______
 you wich to change your enviroment     capital |        | data   |         |
but after you log off.It sets to              othello  starwars letter letter1
default.
```

the /unix-is the kernal
/etc - contains system administrators files,Most are not available to the regular user.(this directory contains the /passwd file)

Here are some files under /etc directory:
/etc/passwd

```
    /etc/utmp
    /etc/adm/sulog
    /etc/motd
    /etc/group
    /etc/conf
    /etc/profile

/dev - contains files for physical devices such as printer and the disk drives
/tmp - temporary file directory
/lib - dirctory that contains programs for high level languages
/usr - this directory contains dirctories for each user on the system

     Eg. of a list of files under /usr
    /usr/tmp
    /usr/lib
    /usr/docs
    /usr/news
    /usr/spool
    /usr/spool/lp
    /usr/lib/uucp

/bin - contain executable programs (commands)

The root also contains:
/bck - used to mount a back up file system.
/install - Used to install and remove utilities
/lost+found - This is where all the removed files go,This dir is used by fsck
              (1M)
/save -A utility used to save data
/mnt - Used for temporary mounting

**Now the fun part scouting around**

                 Local commands (Explained in details)
                 -------------------------------------
At the unix prompt type the pwd command-it will show you the current working
directory you are in.

$ pwd
$ /usr/admin - assuming that you have hacked into a super user acc checkfsys
$

This gives you the full login directory.The / before tell you the location
of the root directory

or

(REFER TO THE DIAGRAM ABOVE)
$ pwd
$ /usr/john
$
Assuming you have hacked into johns acc.

Now lets say you wanted to move down to the michelle directory( you own this)
that contains letters.You would type in

$ cd michelle or cd usr/john/michelle
$ pwd
$ /usr/john/michelle
$

Going back one directory up type in:
$ cd ..
or going to your parent directory just type in "cd"
```

Listing file directories assuming you are in the parent directory:

```
$ ls /usr/john
mail
pers
games
bin
michelle
```

This wont give you the .profile file .To view it type

```
$ cd
$ ls -a
:
:
.profile
```

To list file names in michelles directory type in:

```
$ ls michelle (that if your in the johns directory)
$ ls /usr/john/michelle(parent dir)
```

ls -l

The ls -l is an an important command in unix.This command displays the whole directory in long format :Run this in parent directory

```
$ ls -l
total 60
-rwxr-x---    5 john      bluebox    10 april 9  7:04  mail
drwx------    7 john      bluebox    30 april 2  4:09  pers
     :            :         :         :     :      :    :
     :            :         :         :     :      :    :
-rwxr-x---     6 cathy    bluebox    13 april 1  13:00 partys
     :            :         :         :     :      :    :
$
```

The total 60 tells one the ammount of disk space used in a directory.The -rwxr-x--- is read in triples of 3.The first chracter eg(-,d,b,c)-means as follows: - is an ordinary file ,d is a directory,b is block file,c is a chracter file.
The r stands for read permission,w is write permission,x is execute.The first colum is read in 3 triples as stated above.The first group of 3 (in -rwxr-x---) after the "-" specifies the permission for the owner of the file,the second triple are for the groups (the fourth colum) and the last triple are the permissions for all other users.Therefore the -rwxr-x--- is read as follows. The owner john has permission to read,write and execute anything in the bin directory but the group has no write permission to it and the rest of the users have no permission at all.The format of one of the lines in the above output is as follows:

file type-permissions,links,usersname,group,bytes taken,date,time when last renued,directory or file name.
You will be able to read,execute cathys file named party due to the same group*

chmod

The chmod command changes permission of a directory or a file.Format is
chmod who+,-,=r,w,x
The who is substituted by u-user,g-group,o-other users,a-all.
The + means add permission,- means remove permission,= - assign.
Example :If you wanted all other users to read the file name mail ,type:

```
$ chmod o+r mail
```

cat

Now suppose you wanted to read the file letter .There are teo ways to doing this.First go to the michelle directory then type in:

```
$ cat letter
line one ...\
line two ... }the output of letter
line three../
$
```

or

If you are in the parent directory type in:

```
$ cat /usr/john/michelle/letter
```

and you will have the same output.

Some cat options are -s,-u,-v,-e,-t

Special Chracters in Unix:
---
* - matches any number of single characters eg. ls john* will list all files that begin with john
[...] - matchs any one of the chracter in the [ ]
? - matches any single chracter
runs a process in the backgroung leaving your terminal free
$ - Values used for variables also $n - null argument
> - redirectes output
< - redirects input to come from a file
>> - redirects command to be added to the end of a file
| - pipe output (eg:who|wc-l tells us how many users are online)
"..." - Turn of meaning of special chracters excluding $,`
`...` - allows command output in to be used in a command line
'...' - turns of special meaning of all chracters

continuation of local commands...[   ] -contains the options used
---
passwd

Password changing seems to be a big thing among the savants.Anyway to change the password one would use the 'passwd' command as shown below:

```
$passwd
Changing password for john
Old password:
New password:
Retype new password:
$
```

This will only work when the password has aged enough

ps
--
Its sometimes necessary to see what command procesess you are running,this command lets you see that.
ps [-a all processes except group leaders] [-e all processes] [-f the whole list]

```
$ps
PID   TTY  TIME   COMMAND
200   tty09 14:20  ps
```

The systems reports (PID - process idenetification number which is a # from 1-30,000 assigned to UNIX processes)
It also reports the TTY,TIME and the COMMAND being executed at the time.
To stop a process enter :

```
   $kill [PID] (this case its 200)
   200 terminated
   $
```

grep

This comand is important when seaching for a word or words in large files.

```
grep [argument] [file name] - searchs for an file that contains the argument
                              for example:
   $ grep phone cathy
    phone   michelle  (718)5551234
    phone   cindy   (718)5553456
```

What this did was to find the argument 'phone' in the file cathy.If the argument consists of two or more words then it must be enclosed in single quotes.

mv
--
```
mv [file names(s)] [ dir name ] - renames a file or moves it to another
                                  directory eg.
   $mv letter letters
   $
   This renames the file letter to letters thereby deleting letter
                   or if you want to move files then
   $mv /usr/john/pers/capital /usr/john/michelle/capital
   $
   This moves the file capital to the directory named michelle
```

diff

```
diff [file name] [ file name] - show diffrence between two files.Output of this
                                will have something like 4,5c4,5 then the it
                                will display both sets of files on the screen
                                The 4,5c4,5 means that you must change "c"
                                lines 4 to 5 in one file to line 4 to 5 in
                                another.
      Option for using this command are :
       -b  -  it ignores blank spaces
       -h  - compares it quickly
       -s  - reports files that are the same
       -S[file] - this is when you want to compare a directory starting at a
                  specific file
```

There is also a command to compare 3 files which is :

```
       diff3 [options] [file1] [file2] [file3]
```

cp
--
```
cp [file name] [file name] - makes a copy of a file

   $ cp letter letters
   $
   The file letters is a dupilcate copy of letter.In this case the original
   is not erased like in the mv command
```

.... more UNIX commands:

---

man [command] or [c/r] -will give you a list of commands explainations

help - available on some UNIX systems

mkdir [dir name(s)] - makes a directory

rmdir [dir name(s)] - removes directory.You wont be able to remove the
directory if it contains files in them

rm [file name(s)] - removes files. rm * will erase all files in the current
dir.Be carefull you!!.Some options are :
[-f unconditional removal] [-i Prompts user for y or n]

write [login name] - to write to other logged in users.Sort of a chat

mesg [-n] [-y] - doesn't allow others to send you messages using the write
command.Wall used by system adm overrides it.

$ [file name] - to execute any file

wc [file name] - Counts words,chracters,lines in a file

stty [modes] - Set terminal I/O for the current devices

sort [filename] - Sorts and merges files many options

spell [file name] > [file name] - The second file is where the misspelt words
are entered

date [+%m%d%y*] [+%H%%M%S] - Displays date acoording to options

at [-r] [-l] [job] - Does a specified job at a specified time.The -r Removes
all previously scheduled jobs.The -l reports the job #
and status of all jobs scheduled

write [login] [tty] - Sends message to the login name.Chat!

su [login name]

The su command allows one to switch user to a super user to a user.Very
important could be used to switch to super user accounts.
Usage:

$ su sysadm
password:

This su command will be monitored in /usr/adm/sulog and this file of all files
is carefully monitered by the system administrator.Suppose you hacked in johns
account and then switched to the sysadm account (ABOVE) your /usr/adm/sulog
entry would look like:

SU 04/19/88 21:00 + tty 12 john-sysadm

Therfore the S.A(system administrator) would know that john swithed to sysadm
account on 4/19/88 at 21:00 hours

Searching for valid login names:

Type in-
$ who (command informs the user of other users on the system)

```
cathy  tty1  april 19  2:30
john   tty2  april 19  2:19
dipal  tty3  april 19  2:31
:
:
```
tty is the users terminal,date,time each logged on.dipal,john are valid logins.

Files worth concatenating(cat)
/etc/passwd file:

The etc/passwd is a vital file to cat.For it contains login names of all users including super user accounts and there passwords.In the newer SVR3 releases they are tighting their security by moving the encrypted passwords from /etc/passwd to /etc/shadow making it only readable by root. This is optional offcourse.

```
$ cat /etc/passwd
root:D943/sys34:0:1:0000:/:
sysadm:k54doPerate:0:0:administration:usr/admin:/bin/rsh
checkfsys:Locked;:0:0:check file system:/usr/admin:/bin/rsh
:
other super user accs.
:
john:chips11:34:3:john scezerend:/usr/john:
:
other users
:
$
```
If you have reached this far capture this file as soon as posible.
This is a typical output etc/passwd file.The entries are seperated by a ":".There made be up to 7 fields in each line.
Eg.sysadm account.
The first is the login name in this case sysadm.The second field contains the password.The third field contains the user id."0 is the root".Then comes the group id then the account which contains the user full name etc .The sixth field is the login directory defines the full path name of the the particlar account and the last is the program to be executed.
Now one can switch to other super user account using su command descibed above.
The password entry in the field of the checkfsys account in the above example is "Locked;". This doesn't mean thats its a password but the account checkfsys cannot be accessed remotely.The ";" acts as an unused encryption chracter.A space is also used for the same purpose.You will find this in many UNIX systems that are small systems where the system administrator handles all maintaince.

Password aging:

If password aging is active the user is forced to change the password at regular intervals.One may be able to tell just by looking at the /etc/passwd file when the password is allowed to be changed and when it is compulsory to change it.
For example the entry:

```
john:chips11,43:34:3:John Scezerend:/usr/john:
```

The password contains an extension of (,43) which mean that john can change has to change the password atleast evert 6 weeks and can keep it for atleast 3 week.The format used is [password],Mmww.The M is the maxiumum number of weeks password has to be change and m is the minimum interval password can be changed and the ww is indicates when the password was last changed.

```
    Aging chart:
---------|-----------
```

Character	# of weeks
.	0
/	1
0-9	2-11
A-Z	12-37
a-z	38-63

From the above anyone can determine the number of weeks one can chnage the password.

The (ww) is automatically added as to when the password was last changed .

IF SHAWDOWING IS ACTIVE:

If the shawdowing is active the /etc/passwd would look like this:

```
root:x:0:1:0000:/:
sysadm:x:0:0:administration:/usr/admin:/bin/rsh
```

The password filed is substituted by "x".

The /etc/shawdow file only readable by root will look similar to this:

```
root:D943/sys34:5288::
:
super user accounts
:
Cathy:masai1:5055:7:120
:
all other users
:
```

The first field contains users id:the second contains the password(The pw will be NONE if logining in remotely is deactivated):the third contains a code of when the password was last changed:the fourth and the fifth contains the minimum and the maximum numbers of days for pw changes(Its rare that you will find this in the super user logins due to there hard to guess passwords)

/etc/options directory

The etc/options dir will consists of utilities available in the system.
Example:
```
-rwxr-xr-x   1 root  sys   40 april  1:00  uucp.name
```
uucp standing for BNU

/etc/group

The file has each group on the system.Each line will have 4 entries separated by a ":" . Example of concatenated /etc/group:

```
root::0:root
adm::2:adm,root
bluebox::70:
```

Group name:password:group id:login names
** It very unlikely that groups will have passwords assigned to them **
The id "0" is assigned to /

Sending and recieving messages:

Two programs are used to manage this.They are mail & mailx.The difference between them is that mailx is more fancier thereby giving you many choices like replying message ,using editors etc.

Sending:

The basic format for using this command is:

```
$mail [login(s)]
(now one would enter the text
after finishing enter "." a period
on the next blank line)
$
```

This command is also used to send mail to remote systems.Suppose you wanted to send mail to john on a remote called ATT01
you would type in:

```
$mail ATT01!john
```

Mail can be sent to several users,just by entering more login name after issuing the mail command

Using mailx is the same format:(This I'll describe very briefly)

```
$mailx john
subject:(this lets you enter the subject)
(line #1)
(line #2)
```

(After you finish enter (~.) not the brackets offcourse ,more commands are available like ~p,~r,~v,~m,~h,~b etc.)

Receiving:

After you log on to the system you will the account may have mail waiting.
You will be notified "you have mail".
To read this enter:

```
$mail
(line #1)
(line #2)
(line #3)
?
$
```

After the message you will be prompted with a question mark.Here you have a choice to delete it by entering d,saving it to view it later s,or just press enter to view the next message.
(DONT BE A SAVANT AND DELETE THE POOR GUYS MAIL)

Super user commands:

```
$sysadm adduser - will take you through a routine to add a user
                  (may not last long)
```

Enter this:

```
$ sysadm adduser
password:
(this is what you will see)
/-------------------------------------------------------------------------\
  Process running succommmand `adduser`
  USER MANAGMENT

  Anytime you want to quit, type "q".
  If you are not sure how to answer any prompt, type "?" for help

  If a default appears in the question,press <RETURN> for the default.
```

```
  Enter users full name [?,q]: (enter the name you want)
  Enter users login ID [?,q]:(the id you want to use)
  Enter users ID number (default 50000) [?,q) [?,q]:( press return )
  Enter group ID number or group name:(any name from /etc/group)
  Enter users login home directory:(enter /usr/name)

  This is the information for the new login:
  Users name: (name)
  login ID:(id)
  users ID:50000
  group ID or name:
  home directory:/usr/name
 Do you want to install,edit,skip [i,e,s,q]? (enter your choice if "i" then)
 Login installed
 Do you want to give the user a password?[y,n] (its better to enter one)
 New password:
 Re-enter password:

 Do you want to add another login?
\-----------------------------------------------------------------------------/
```

This is the proccess to add a user.Since you hacked into a super user account you can make a super user account by doing the following by entering 0 as an user and a group ID and enter the home directory as /usr/admin.This will give you as much access as the account sysadm
Caution - Do not use login names like Hacker,Cracker,Phreak etc .This is a total give away.
The process of adding a user wont last very long the S.A will know when he checks out the /etc/passwd file

$sysadm moduser - This utility allows one to modify users.DO NOT ABUSE!!!
Password:

This is what you'll see:

```
/-----------------------------------------------------------------------------\
MODIFYING USER'S LOGIN

1)chgloginid  (This is to change the login ID)
2)chgpassword (Changing password)
3)chgshell (Changing directory DEFAULT = /bin/sh)

ENTER A NUMBER,NAME,INITIAL PART OF OF NAME,OR ? OR <NUMBER>? FOR HELP,
Q TO QUIT ?
\-----------------------------------------------------------------------------/
```

Try every one of them out.Do not change someones password.It creates a havoc.
If you do decide to change it.Please write the original one down somewhere and change back.Try not to leave to many traces after you had your fun.
In choice number 1 you will be asked for the login and then the new one.
In choice number 2 you will asked for the login and then supplied by it correct password and enter a new one.
In choice 3 this is used to a pchange the login shell ** Use full **
The above utilites can be used separatly for eg(To change a password one coulfd enter: $sysadm chgpasswd not chapassword ,The rest are same)

$sysadm deluser - This is an obviously to delete a user
password:

This will be the screen output:

```
/-----------------------------------------------------------------------------\
Running subcommand 'deluser' from menu 'usermgmt'
USER MANAGEMENT
This fuction completely removes the user,their mail file,home directory
```

and all files below their home directory from the machine.

```
Enter login ID you wish to remove[q]:      (eg.cathy)
'cathy' belongs to 'Cathy Franklin'
whose home directory is /usr/cathy
Do you want to remove this login ID 'cathy' ? [y,n,?,q] :

/usr/cathy and all files under it have been deleted.

Enter login ID you wish to remove [q]:
\-----------------------------------------------------------------------/
```

This command deletes everthing owned by the user.Dont use it even if you have access to it.

other super user commands:

```
wall [text] control-d  - to send an anouncement to users logged in(will
                         override mesg -n command).Execute only from /
/etc/newgrp - is used to become a member of a group

sysadm [program name]
        delgroup - delets groups
        whoson - self explanatory
        lsgroup - Lists group
        mklineset -hunts various sequences
        lsuser -lists all the users & their logins names
```

Other commands may require file system to be mounted.

Basic Networking utility(BNU)

The BNU is a unique feature in UNIX.Some systems may not have this installed. What BNU does is allow other remote UNIXes communicate with yours without logging off the present one.BNU also allowes file transfer between computers. Most UNIX systems V will have this feature installed.

The user program like cu,uux etc are located in the /usr/bin directory

Basic Networking Files:

```
/usr/lib/uucp/[file name]
 [file name]
 systems - cu command to establishes link.Contains info on remote computers
           name,time it can be reached,login Id,password,telephone numbers
 devices - inter connected with systems files(Automatic call unit same in two
           entries)also cantains baud rate,port tty1 etc.

 dialers - where asscii converation must be made before file tranfers etc.
 dialcodes - contains abreiviations for phone numbers that can be used in
             systems file

 other files are sysfiles,permissions,poll,devconfig
```

B.N.U Aministrative files:

There are 5 admnistrative files present.These are files are created in the /usr/spool directory .These A.Files are responsible for various BNU procceses like kepping records data ,files tranfers bettwenn remote and local and also usefull to lock devices.

TM - This file used to hold temporary data .When tranfering the files from a remote to local the /usr/spool/uucp/[name of the remote computer] creates this in the format of as of below:

TM[Process Identification Number].[ddd]

The ddd is the a 3 digit number (sequential) starting with "0"
Here a typical eg: TM322.012
Then this file is moved into the path defined by the C.sysnxxx file

X.[Execute files] - Created in the /usr/spool before you execute the commands in remote.
The format used to name this file is X.sysnxxx
where sys stand for the remote name and n is the priority level the xxxx is a sequence assingned by the uucp.These files always contain the Name of the file ,Comuter & file name to recieve,Persons login & computer name and the command string.

LCK - The lock file created in the /usr/spool/locks directory.The is used when devices are being used.Prevent usage of the same calling device.

Format used: LCK.str wher the str is a device name.The Lock file contains the PID needed to lock

C.sysnxxx - created in the usr/spool directory.These are the work files.Used when work is in line,remote execeutions.Format is same as the X.sysnxxxx.The works files contain the full path name of the file to be sent,path name of the destination (TM Transfers),Remote login name to be notified after the file transmision is complete,Users login name and the name of the programs used eg.uucp,uupick etc.

D - The data files.Format used is D.systmxxxxyyy.These files are created when specified in a command to copy to the spool directory.Eg. By the usage of uucp -C this will be true.
The systm is the remote name,xxxx is the the 4 digits seq assingned by the uucp.The yyy is a sub sequence number.

Logining on to remote and sending+receiving files
---

cu - This command allows one to log on to the local as well as the remote Unix (or a non unix)without haveing to hang up so you can transfer files.
Usage:[options]

```
$ cu [-s baud rate][-o odd parity][-e even parity][-l name of comm line]
     telephone number | systemname
```

To view system names that you can communicate with use the 'unname' command:
Eg. of output of names:

```
ATT01
ATT02
ATT03
ATT04
```

```
$ cu -s300 3=9872344 (9872344 is the tel#)
 connected
 login:
 password:
```

local strings:

<~.> - will log you off the remote terminal but not the local

~! - out you on the local withiout disconnecting the line from remote
<control-d> - puts you back on the remote unix
~%take [file name] - takes a copy of the file name and copies it to the
local(the directory which you are in)
"%put [file name] - reverse of above
~$[command] - allows the execution of a command to the local from remote

ct
--
ct allows local to connect to remote.Initiates a getty on a remote terminal.
Usefull when using a remote terminal.BNU has call back feature that allows
the user on the remote who can execute a call back meaning the local can call
the remote.[ ] are options

$ ct [-h prevent automatic hang up][-s bps rate][-wt set a time to call back
abbrieviated t mins] telephone number

uux

To execute commands on a remote (unix to unix)
usage:[ ] are options

$ uux [- use standard output][-n prevent mail notification][-p also use
standard output] command-string

uucp
----
uucp copies files from ones computer to the home directory
of a user in remote system.This also works when copying files from one
directory to another in the remote.The remote user will be notified by mail.
This command becomes use full when copying files from a remote to your local
system.
The uucp requires the uucico daemon will call up the remote and will perform
file login sequence,file transfer and notify the user by mail.
Daemons are programs runining in the background.The 3 daemons in a Unix are
uucico,uusched,uuxqt.

Daemons Explained:[nows a good time to explain the 3 daemons]
---

uuxqt - Remote execution.This daemon is executed by uudemon.hour started by
cron.UUXQT searchs in the spool directory for executable file
named X.file sent from the remote system.When it finds a file X.file
where it obtains process which are to be executed.The next step is
to find weather the processes are available at the time.The if
available it checks permission and if everthing is o.k it proceeds
the background proccess.

uucico - This Daemon is very immportant for it is responsible in establishing
a connection to the remote also checks permission,performs login
procedures,transfers + executes files and also notifies the user
by mail.This daemon is called upon by uucp,uuto,uux commands.

uusched - This is executed by the shell script called uudemon.hour
This daemons acts as a randomizer before the UUCICO daemon is
called.

Usage of uucp command:

$ uucp [options] [first full path name!] file [destination path!] file
example:
$ uucp -m -s bbss hackers unix2!/usr/todd/hackers

What this would do is send the file hackers from your computer to the remotes /usr/todd/hackers making hackers offcourse as file.todd would mail that a file has been sent to him.The unix2 is the name of the remote.
Options for uucp:(Dont forget to type in remotes name unix2 in case)
-c dont copy files to spool directory
-C copy to spool
-s[file name] - this file will contain the file status(above is bbss)
-r Dont start the comm program(uucico) yet
-j print job number(for above eg.unix2e9o3)
-m send mail when file file is complete

Now suppose you wanted to receive file called kenya which is in the usr/dan/usa to your home directory /usr/john assuming that the local systems name is ATT01 and you are currently working in /usr/dan/usa,you would type in:

$uucp kenya ATT01!/usr/john/kenya

uuto

The uuto command allows one to send file to remote user and can also be used to send files locally.
Usage:
$ uuto [file name] [system!login name](omit systen name if local)

Conclusion:

Theres always more one can say about the UNIX but its time to stop.
I hope you have enjoyed the article.I apologize for the lenght. I hope I made the UNIX operating system more familiar.
Remember do not abuse any systems you hack into for a true hacker doesn't like to reck but to learn.
I can be reached at (718)358/9209 - Hackers Den88 [2600 BBS #5]

Watch for my new article on using PANAMAC airline computers coming soon.

Red Knight
P/HUN!
<<T.S.A.N>>

Leached off SSC (713) 497-2312

[13] [UNIX system specifics (all versions)]
(98) Minutes Remaining
(G-Files Menu) Command <?-Help>: [

X-=-=-=